2. What are the different types of vulnerabilities (software, hardware, network)?

Cybersecurity vulnerabilities can be broadly categorized based on the type of system or asset affected. Here's a breakdown of **software**, **hardware**, and **network vulnerabilities**, along with examples for clarity:

---

1. Software Vulnerabilities

Flaws or weaknesses in code, design, or configuration of software applications.

Types:

- **Buffer Overflow:** When a program writes data beyond allocated memory, potentially allowing attackers to inject malicious code.
  - Example: **CVE-2017-5638** in Apache Struts exploited in the Equifax breach.
- **SQL Injection:** Injecting malicious SQL queries to manipulate or access databases.
  - Example: Exploiting login forms or search bars.
- **Cross-Site Scripting (XSS):** Injecting scripts into web pages viewed by other users.
  - Example: Persistent XSS in comment sections of websites.
- **Unpatched Software:** Failing to update software leads to exploitation of known vulnerabilities.
  - Example: The **WannaCry ransomware** exploited a Windows SMB protocol vulnerability.

---

2. Hardware Vulnerabilities

Weaknesses in physical devices or their firmware that attackers can exploit.

Types:

- **Firmware Vulnerabilities:** Outdated or insecure firmware allows unauthorized control.
  - Example: Firmware-level attacks like **TrickBot** targeting IoT devices.
- **Side-Channel Attacks:** Exploiting physical properties (e.g., power usage or timing) to extract sensitive data.
  - Example: **Spectre** and **Meltdown** targeting CPU flaws.
- **Supply Chain Attacks:** Malicious components or code injected during manufacturing.
  - Example: **Supermicro hardware implants**.
- **Lack of Secure Boot:** Devices without proper authentication mechanisms can load malicious software at startup.

3. Network Vulnerabilities

Weaknesses in the design, configuration, or security of network systems.

Types:

- **Man-in-the-Middle (MITM):** Intercepting or altering communication between two parties.
  - Example: Exploiting unsecured HTTP connections.
- **DNS Spoofing/Poisoning:** Redirecting traffic to malicious sites by altering DNS records.
  - Example: Redirecting users to phishing sites.
- **Weak Wi-Fi Encryption:** Using outdated protocols like WEP or weak WPA keys.
  - Example: **KRACK attack** on WPA2 encryption.
- **Open Ports:** Unsecured or unused ports can allow unauthorized access.
  - Example: Exploitation of **port 3389 (RDP)** for remote attacks.
- **DDoS Attacks:** Exploiting inadequate protections against traffic overloads.
  - Example: The **Mirai botnet** targeting IoT devices.

Comparison Table

Type	Focus	Examples	Prevention
Software	Applications	Buffer Overflow, XSS	Patching, Secure Coding Practices
Hardware	Physical Devices	Spectre, Firmware Attacks	Secure Boot, Firmware Updates
Network	Connectivity	MITM, DNS Spoofing, DDoS	Firewalls, Encryption, Monitoring

---